fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения: 10.10.2013).

2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации : утв. решением председателя Гос. техн. комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс]. Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения: 10.10.2013).

3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации : утв. решением председателя Гос. техн. комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс]. Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения: 10.10.2013).

4. Защита от несанкционированного доступа к информации. Ч. 1: Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей: утв. решением председателя Гос. техн. комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114. [Электронный ресурс]. Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения: 10.10.2013).

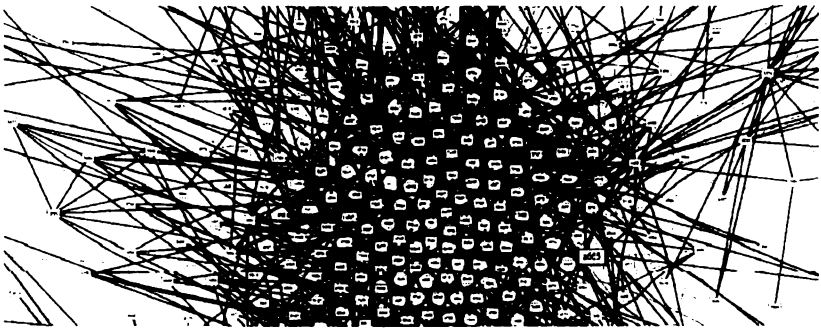
5. Система защиты информации от несанкционированного доступа «СТРАЖ NT» Версия 3.0. Описание применения. 2010 г. [Электронный ресурс]. Режим доступа: http://guardnt.ru/download/doc/app_guide_nt_3_0.pdf (дата обращения: 10.10.2013).

РАЗВИТИЕ MESH-СЕТЕЙ С ПОМОЩЬЮ МОБИЛЬНЫХ УСТРОЙСТВ

Н. А. Токарчук, А. Н. Соколов
(Челябинск, ЮУрГУ (национальный исследовательский университет), conference+urfu@mainnika.ru)

Современные глобальные компьютерные сети, несмотря на все свои преимущества, имеют существенный недостаток – они централизованы. Если выключается один узел связи – все те, кто был через него подключен, теряют связь. Общество сегодня слишком зави-

сит от наличия доступа в Интернет, чтобы допускать подобное. Идея mesh-сетей (сети с ячеистой топологией) состоит в том, чтобы создать «острова» децентрализованных сетей, например улицы, или, в более больших масштабах, целые города, которые сначала будут соединены между собой через существующую сетевую инфраструктуру и при наличии технической возможности тоже будут объединены в децентрализованную сеть (рисунок). Создавать подобные «острова» становится возможным с помощью современных беспроводных компьютерных сетей, благодаря их распространенности.



Фрагмент карты сети hyperboria
в случайный момент времени

Проект сети hyperboria ставит перед собой целью создание приватной децентрализованной mesh-сети для всех желающих. Чтобы каждый человек, даже далекий от информационных технологий, смог установить программу и начать ей пользоваться сразу, не вникая в подробности работы сети. Hyperboria основывается на программном обеспечении cjdns. Принцип работы сети следующий: весь трафик между клиентом и сервером зашифрован с помощью асимметричного шифрования, трафик между отдельными надами также шифрован. Маршруты в сети строятся с помощью децентрализованных хэш-таблиц (DHT), отдельная нода не хранит сведения обо всех маршрутах сети. Путь для трафика выбирается через самую короткую цепочку нодов. Сеть работает через протокол IPv6, клиентам выдается публичный IPv6-адрес из приватной части.

Работа hyperboria в режиме mesh осуществляется с помощью беспроводных сетей. В настоящий момент сеть в режиме mesh может работать только через модифицированные беспроводные точки доступа. Цель моей работы состоит в том, чтобы расширить и облегчить распространение hyperboria за счет портирования и модифицирования программы cjdns для работы под операционной системой Android. Результат работы (документация, исходный код) опубликован под открытой лицензией GNU GPLv3 (GNU General Public License).

Первым этапом разработки является портирование ядра роутера. На этом этапе осуществляется сборка программы роутера и зависимостей, учитывая нюансы операционной системы android. В качестве компилятора используется Android NDK (Native Development Kit). Стоит отметить, что уже на данном этапе сеть может начать работу на мобильном устройстве. Пользователям сети нужно учитывать следующие особенности и ограничения:

- работа программы cjdns только на версиях android с полным root-доступом;
- запуск программы осуществляется только через отладочную консоль устройства;
- необходимость наличия модулей ядра в устройстве для создания туннельного интерфейса;
- необходимость ручного создания туннельного интерфейса, на разных моделях устройств путь до системного файла /dev/net/tun может отличаться;
- невозможность автоматического поиска нодов через wi-fi.

На *втором этапе разработки* модифицируется сетевая часть. Данный этап является одним из самых важных. Во-первых, отделение сетевой платформозависимой части (создание и использование туннельного интерфейса) позволит избавиться от некоторых ограничений, которые были озвучены на предыдущем этапе. Во-вторых, это предоставит удобство использования конечному пользователю, так как для работы не будет требоваться наличие прав администратора на устройстве, и позволит одним нажатием установить приложение из магазина Play Market (магазин приложений, с которым по умолчанию работает операционная система Android).

При реализации этапа API Android, который позволяет создавать пользовательские VPN-сети (VpnService.Builder). После создания интерфейса его файловый дескриптор android.os.ParcelFileDescriptor отделяется методом detachFd() и передается в ядро роутера, которое продолжает работать с ним дальше.

API Android позволяет создать приложение-обертку, которое предоставит пользовательский интерфейс со статусом подключения к сети, информацией о трафике, уведомлениями о нарушениях работы. Приложение запускается обычным образом, как и любое другое, без каких-либо особенностей. Ограничение на данном этапе остается только одно – невозможность автоматического поиска нод через wi-fi.

На *третьем этапе* раскрывается вся мощность работы сети в mesh-режиме. Мобильное устройство само будет искать доступные для подключения ноды, осуществлять контроль, принимать подключения от других нод. Работа по данному этапу только планируется, потому что здесь нужно очень подробно рассмотреть множество факторов, начиная от возможностей операционной системы Android и заканчивая быстрым физическим перемещением нодов.

В заключение следует отметить, что hyperboria – это простая, но в то же время мощная сеть для обмена информацией в защищенном режиме. Зона покрытия зависит от количества устройств, которые подключены к ней. Подключение мобильных устройств к сети позволит каждому пользователю иметь приватный канал доступа, защищенный асимметричными алгоритмами шифрования. Еще одним плюсом работы сети в режиме mesh является простота организации подключения. Например, даже в ситуациях, когда работа обычных сетей связи невозможна (техногенные, природные катастрофы, и т. п.), hyperboria позволит оставаться на связи для получения сведений и помощи.